AKTUALITY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Správa (september – október 2025)

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-0002.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

Vážení čitatelia, týmto vám predstavujeme správy o aktuálnom vývoji v oblasti regulácie kybernetickej bezpečnosti. Cieľom týchto správ je poskytnúť prehľad nových vedeckých článkov, monografií a iných odborných zdrojov, ktoré ovplyvňujú implementáciu povinností vyplývajúcich z európskej aj národnej legislatívy, ako aj identifikovať výskumné a aplikačné trendy v praxi.
V súčasnej digitálnej dobe predstavuje kybernetická bezpečnosť nevyhnutnú súčasť ochrany štátu, verejnej správy a kritickej infraštruktúry. Vzhľadom na rastúci počet kybernetických útokov a zvyšujúce sa požiadavky na bezpečnosť informačných systémov boli a budú potrebné zmeny právnej úpravy v tejto oblasti. Táto správa preto zhromažďuje najnovšie odborné a vedecké publikácie za posledné obdobie.

ČO JE NOVÉ V OBLASTI KYBERNETICKEJ BEZPEČNOSTI?

Kybernetické incidenty

Kybernetický útok zameraný na systém check-in a boarding systémov poskytovaných firmou Collins Aerospace spôsobil rozsiahle zmeny v prevádzke viacerých európskych letísk, vrátane London Heathrow, Brussels Airport a Berlin Airport, čo viedlo k meškaniam, zrušeniam letov a dlhým frontám cestujúcich. Útok sa začal v noci 19. septembra 2025 a jeho následky sa prejavili počas nasledujúcich dní, keď museli prevádzky prejsť na manuálne odbavovanie pasažierov pri check-ine a nadväzujúcich procesoch. Určenie pôvodu útoku zostalo spočiatku nejasné, no incident opäť zvýraznil zraniteľnosť leteckých dodávateľských reťazcov a zdieľaných IT systémov voči kybernetickým hrozbám.

Reuters priniesol správy o úniku údajov zákazníkov automobilky Stellantis. Tá oznámila, že neautorizovaný prístup k platforme jej tretieho poskytovateľa, ktorý podporuje zákaznícke služby pre Severnej Amerike, viedol k úniku osobných kontaktov zákazníkov. Spoločnosť uviedla, že incident nepostihol jej interné systémy, ale ovplyvnil platformu externého partnera a bol objavený pri monitorovaní bezpečnosti. Kompromitované mali byť len „kontaktné informácie" zákazníkov, napríklad mená a e-mailové adresy, a žiadne finančné či citlivé osobné údaje neboli uložené ani prístupné na tejto tretej platforme.

Spoločnosť spustila reakčné protokoly, vyšetrovanie a upozornila príslušné orgány, zároveň informuje dotknutých zákazníkov a vyzýva ich k opatrnosti voči phishingovým útokom. Portál Techradar k tomu dodáva, že informácie z niektorých bezpečnostných reportov naznačujú, že incident môže byť súčasťou širšej kampane zneužitia databáz Salesforce, pri ktorej skupina ShinyHunters tvrdí, že získala milióny záznamov z rôznych podnikov, vrátane údajov o zákazníkoch. Stellantis zatiaľ nepotvrdil tieto tvrdenia.

Skupina hackerov tvrdí, že ukradla takmer miliardu záznamov uložených zákazníkmi Salesforce. Skupina ohlásila, že získala takmer 1 miliardu záznamov od spoločností používajúcich cloudový softvér Salesforce. Skupina sa označuje ako „Scattered LAPSUS$ Hunters" a uviedla, že údaje obsahujú osobne identifikovateľné informácie. Na a dark-webovom leak webe zverejnila zoznam približne 40 spoločností, o ktorých tvrdí, že boli kompromitované, hoci nie je jasné, či všetky tieto firmy skutočne používajú Salesforce alebo či došlo k overenému úniku. Jeden z členov, ktorý sa identifikoval ako „Shiny", povedal Reuters, že neprišli priamo cez hackovanie samotného

Salesforce, ale cieľili na používateľské organizácie, kde pomocou vishingu oklamali personál IT helpdesku, aby získali prístup k účtom alebo nástrojom ako Data Loader. Potvrdzuje to aj vyjadrenie spoločnosti, ktorá odmieta, že by došlo k prelomeniu jeho platformy alebo zraniteľnosti v technológii, a tvrdí, že neexistuje žiadny dôkaz kompromitácie samotnej služby. Útočníci podľa ich vyjadrení cílené na zákazníkov Salesforce prostredníctvom sociálneho inžinierstva, konkrétne tzv. *vishingu* (hlasový phishing), pri ktorom sa snažia oklamať zamestnancov a získať prístup k dátam.

Organizácia Noyb sídliaca v Rakúsku priniesla vážne zistenia ohľadom Microsoftu 365, v dôsledku čoho podala sťažnosť na rakúsky úrad pre ochranu osobných údajov. Ten zistil, že Microsoft 365 Education nezákonne sledoval žiakov a porušil tak GDPR. Používal tracking cookies bez súhlasu používateľov, čo DSB označil za nezákonné spracúvanie osobných údajov. Spoločnosť teraz musí zmazať príslušné osobné údaje a poskytnúť prístup k údajom používateľa v súlade s článkom 15 GDPR. Údaje žiakov boli tiež použité pre obchodné účely bez právneho základu, v dôsledku čoho bude musieť Microsoft jasne vysvetliť, ako používa údaje pre svoje obchodné účely (ako napríklad „business modeling" či „energy efficiency") a či údaje odoslal tretím stranám vrátane LinkedIn, OpenAI či sledovacej firmy Xandr.

Európska komisia 15. mája 2025 oznámila predbežný záver, že sociálna sieť TikTok nezabezpečila primerané zverejňovanie údajov o reklame a platenej komerčnej komunikácii, ako to vyžaduje Digital Services Act (DSA). Podľa Komisie TikTok neplní povinnosť sprístupniť úplné a presné údaje o svojej reklamnej databáze, ktorá by umožnila externým výskumníkom, orgánom a verejnosti transparentne a legitímne analyzovať platby reklám a ich cielenie. Databáza neobsahuje všetky povinné informácie, neumožňuje spoľahlivé vyhľadávanie ani analýzu reklám a nie je navrhnutá tak, aby ju mohli efektívne používať výskumníci, občianska spoločnosť a orgány dohľadu

Predbežné zistenie znamená, že TikTok môže byť nariadením DSA donútený rozšíriť a vylepšiť svoju transparentnosť reklám, inak mu hrozia pokuty do výšky % z celosvetového obratu, ktoré sú podľa DSA navrhnuté tak, aby odradzovali od neplnenia pravidiel.

Rozhodnutie potvrdzuje, že formálne splnenie povinností nestačí — Komisia bude hodnotiť reálnu použiteľnosť a kvalitu nástrojov transparentnosti. Pre technologické firmy to znamená potrebu prepracovať interné systémy reklamy, dátovej správy a reportingu, aby obstáli nielen technicky, ale aj z pohľadu verejného dohľadu.

LEGISLATÍVA A SÚDNE ROZHODNUTIA

Ako už názov vypovedá, v tejto časti si rozoberieme novinky z oblasti legislatívy a súdnych rozhodnutí ktoré rezonovali v rámci kybernetického sektora. V prvom rade však poukážeme na legislatívne návrhy viacerých štátov vrátane iniciatív Európskej únie.

Legislatíva

V Slovenskej republike došlo ku viacerým zmenám. Národný bezpečnostný úrad (NBÚ) vydal Metodiku analýzy rizík, ktorá je určená na použitie v procesoch riadenia rizík v súlade s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov.

Zároveň dňa 1. septembra 2025 nadobudli účinnosť dve nové vyhlášky vydané Národným bezpečnostným úradom (NBÚ), ktoré súvisia so zákonom č. 69/2025 Z. z. o kybernetickej bezpečnosti. Išlo o vyhlášku č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hlásení incidentov.

Ako druhá bola prijatá vyhláška č. 227/2025 Z. z. o bezpečnostných opatreniach, ktorá nahrádza predchádzajúcu vyhlášku č. 362/2018 Z. z. a ktorá ustanovuje obsah bezpečnostných opatrení, rozsah všeobecných bezpečnostných opatrení pre siete, informačné systémy a prevádzkové technológie, ako aj obsah a štruktúru bezpečnostnej dokumentácie podľa § 20 zákona o kybernetickej bezpečnosti. Kľúčové body predpisu možno predstaviť nasledovne:

- Definovanie povinných bezpečnostných opatrení: Vyhláška určuje, aké všeobecné bezpečnostné opatrenia musia byť prijaté pre rôzne oblasti kybernetickej bezpečnosti a ako sa tieto opatrenia stanovujú na základe analýzy rizík.

- Bezpečnostná dokumentácia: Predpis konkretizuje, aké dokumenty musia organizácie viesť, vrátane politiky bezpečnosti a záznamov o identifikovaných aktívach a rizikách, pričom vyžaduje, aby dokumentácia reálne odrážala stav procesov a opatrení v organizácii.

- Zameranie na prevádzkovateľov základných služieb: Vyhláška sa vzťahuje na subjekty, ktorým zákon o kybernetickej bezpečnosti ukladá povinnosti, a určuje, ako a v akom rozsahu majú implementovať bezpečnostné opatrenia podľa národnej metodiky.

- Prebratie právnych aktov EÚ: Súčasťou vyhlášky je aj prevzatie relevantných právne záväzných aktov Európskej únie v oblasti kybernetickej bezpečnosti.

Nemecko prijalo nariadenie o diaľkovom riadení cestnej dopravy (Straßenverkehr-Fernlenk-Verordnung), ktoré upravuje diaľkové ovládanie automatizovaných vozidiel. Týmto právnym predpisom sa stanovujú podmienky pre typové schvaľovanie, zodpovednosti prevádzkovateľov a požiadavky na kybernetickú bezpečnosť. Nariadenie vytvára právny základ pre prevádzku motorových vozidiel riadených na diaľku (teleoperovaných) na cestách v Nemecku.

Regulácia umožňuje, aby osoba sediaca mimo vozidla, napríklad v centrálnom ovládacom centre, ovládala vozidlo pomocou diaľkového prístupu, čo predstavuje významný krok vpred pre mobilitu v ére digitalizácie a autonómnych technológií. Od 1. decembra 2025 budú môcť byť motorové vozidlá riadené na diaľku testované a prevádzkované na verejných komunikáciách v rámci päťročnej experimentálnej fázy, s jasne stanovenými podmienkami povolenia a bezpečnostnými požiadavkami.

Nemecko tiež rieši nový návrh spolkového zákona o informačnej bezpečnosti, ktorý implementuje smernicu NIS 2, čím udáva jasný kurz pre posilňovanie kybernetickej bezpečnosti. Podľa § 38 ods. 3 predmetného návrhu zákona (BSIG) je manažment (vedenie) povinný absolvovať školenia zamerané na relevantné kybernetické riziká a postupy v oblasti informačnej bezpečnosti. „Školenie vedenia k NIS 2" [NIS-2-Geschäftsleistungsschulung] má poskytovať predbežné usmernenie a odporúčania k tomuto povinnému vzdelávaniu manažmentu, a to najmä pre inštitúcie, ktorým z nového návrhu zákona vyplývajú povinnosti.

Taliansko sa stalo jednou z prvých krajín EÚ, ktorá prijala národný zákon o umelej inteligencii, upravujúci používanie AI vo verejnej správe aj v súkromnom sektore. Zákon č. 132 z 23. septembra

2025 o umelej inteligencii vytvára komplexný národný rámec pre reguláciu AI a nadväzuje na Európske nariadenie AI Act, pričom jeho ustanovenia nadobudnú účinnosť 10. októbra 2025. Zákon zavádza povinnosti transparentnosti, etické štandardy a konkrétne obmedzenia používania dohľadových technológií. Z hľadiska jeho obsahu možno identifikovať špecifické pravidlá pre kľúčové oblasti:

- zdravotníctvo: AI môže podporovať prevenciu, diagnostiku a liečbu s tým, že konečné rozhodnutia zostávajú v rukách odborníkov;

- trh práce: používanie AI na pracovisku musí zlepšovať podmienky a produktivitu bez diskriminácie a s povinnosťou zamestnávateľov informovať pracovníkov o jeho použití;

- regulované profesie: AI slúži ako nástroj podpory pri intelektuálnych profesiách, no rozhodnutia musia zostať v rukách ľudí;

- verejná správa a justícia: AI je povolená ako podporný nástroj, ale rozhodovanie o aplikácii práva je výlučne v rukách sudcov.

Zákon tiež upriamuje pozornosť aj na autorské práva v kontexte diel vytvorených AI. Tie majú byť chránené iba vtedy, ak odrážajú inteligentnú tvorivú prácu človeka resp. autora. Zavádza aj nové ustanovenia kriminalizujúce nelegálne rozširovanie AI-generovaného obsahu (napr. deepfake), s trestami od 1 do 5 rokov väzenia.

Aj Česká republika predstavila návrh zákona o umelej inteligencii (Zákon o umělé inteligenci), ktorý má zosúladiť národnú legislatívu s EÚ AI Act-om. Návrh počíta so zriadením orgánov dohľadu a zavedením povinností v oblasti súladu (compliance) pri nasadzovaní vysokorizikových systémov AI. Súčasťou zákona sú aj regulačné sandboxy. Uvedený zákon má za cieľ minimalisticky adaptovať len tie aspekty európskeho nariadenia, ktoré si vyžadujú zásah členského štátu (napr. dozorné mechanizmy), pričom hlavné povinnosti a pravidlá pre systémové AI zostávajú v pôsobnosti samotného AI Act-u.

Na nadnárodnej úrovni stojí za pozornosť, že Európska komisia zverejnila návrh usmernenia a šablónu na nahlasovanie pre vysokorizikové systémy umelej inteligencie. Podľa článku 73 Aktu o umelej inteligencii sa musia závažné incidenty hlásiť bezodkladne. Týmto krokom sa uvádza do praxe európsky rámec správy a riadenia AI prostredníctvom zakotvenia zodpovednosti, transparentnosti a nápravných opatrení v rámci celého životného cyklu AI.

V rámci tejto snahy Európska komisia navrhla štandardizovaný formulár, ktorým sa má predísť chaosu, keď každý členský štát vyžaduje iné údaje.
Šablóna by mala obsahovať a) Identifikáciu systému: jedinečné ID systému (ak je registrovaný v databáze EÚ); b) popis incidentu: čo sa stalo, kde, kedy a aké boli následky; c) nápravné opatrenia: čo firma urobila okamžite po zistení chyby (napr. vypla systém, opravila algoritmus); d) analýzu príčin: prečo k zlyhaniu došlo (napr. chyba v tréningových dátach, kybernetický útok, nepredvídané použitie).

Okrem toho Európska komisia a Európsky výbor pre ochranu údajov (EDPB) vydali nový návrh spoločných usmernení na objasnenie vzájomného pôsobenia medzi Aktom o digitálnych trhoch (DMA) a nariadením GDPR. Jeho cieľom je podporiť dodržiavanie predpisov vo všetkých členských štátoch. Európska komisia spolu s EDPB zároveň zverejnili Usmernenia (Guidelines) 3/2025 o súhre

medzi Aktom o digitálnych službách (DSA) a GDPR. Toto usmernenie sa zameriava na zabezpečenie uplatňovania ochrany údajov v rámci DSA, pričom sa týka najmä transparentnosti, spracúvania údajov a zodpovednosti.

Zo zámoria prichádza správa o tom, že štát Kalifornia schválil balík 18 nových zákonov o bezpečnosti umelej inteligencie, ktoré pokrývajú témy ako deepfakes, ochrana údajov a zodpovednosť pri využívaní AI. Stal sa tak prvým americkým štátom, ktorý priamo reguluje bezpečnosť umelej inteligencie. Táto legislatíva tiež vychádza z odporúčaní Spoločnej kalifornskej pracovnej skupiny pre politiku hraničných modelov AI (Joint California Policy Working Group on AI Frontier Models).

Súdne rozhodnutia

Súdny dvor Európskej únie sa nedávno zaoberal konaním C-474/24 (NADA Austria a ďalší), kde generálny advokát uviedol, že zverejňovanie porušení antidopingových pravidiel športovcov na internete je podľa GDPR prípustné len vtedy, ak je primerané a v súlade so zásadami minimalizácie údajov a zodpovednosti.

Hoci antidopingové údaje môžu zahŕňať informácie súvisiace so zdravím alebo kvázi-trestné údaje, ich zverejnenie musí byť odôvodnené legitímnym verejným záujmom a podliehať individuálnemu posúdeniu v každom jednotlivom prípade. Generálny advokát zdôrazňuje, že kombinácia rozsahu, automatizovaného charakteru a verejného sprístupnenia týchto údajov môže zasahovať do ochrany osobných údajov, ak nebola vykonaná individuálna vyvážená analýza záujmov dotknutých osôb.

Generálny advokát zároveň potvrdil, že dotknuté osoby môžu podať sťažnosť aj v prípade, že spracúvanie údajov ešte len hrozí, čím sa umožňuje preventívna ochrana práv podľa GDPR. Aby sme ujasnili kontext tohto sporu, v pôvodnom rakúskom konaní spor vznikol pre povinnosť zverejňovať na webových stránkach NADA Austria a ÖADR informácie o športovcoch, ktorí porušili antidopingové pravidlá. A aj keď názor generálneho advokáta nie je pre súd záväzný, výrazne ovplyvňuje očakávané rozhodnutie súdu vzhľadom na interpretáciu GDPR v kontexte zverejňovania citlivých údajov pri verejných režimoch.

Pri Súdnom dvore EÚ ostaneme aj v prípade Dun & Bradstreet Austria (C-203/22, 27. 2. 2025) týkajúcom sa práva na vysvetlenie pri automatizovanom rozhodovaní.

Spor vznikol z reklamácie zákazníka, ktorému mobilný operátor odmietol uzavrieť zmluvu na základe kreditného skóre vypočítaného spoločnosťou Dun & Bradstreet Austria. Rakúsky súd zistil, že spoločnosť odmietla sprístupniť logiku výpočtu a odvolávala sa na obchodné tajomstvá. SDEÚ rozhodol, že podľa čl. 15 ods. 1 písm. h) Nariadenia Európskeho parlamentu a rady (EÚ) 2016/ 679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len ako „GDPR") musí prevádzkovateľ opísať postup a zásady uplatňované pri automatizovanom rozhodovaní tak, aby jednotlivci mohli pochopiť, ktoré osobné údaje boli použité a ako ovplyvnili rozhodnutie. Tajomstvo algoritmu nie je dôvodom na úplné odmietnutie vysvetlenia, prevádzkovateľ môže zverejniť informácie vo všeobecnej rovine alebo ich poskytnúť súdu, ktorý posúdi rovnováhu medzi právom na vysvetlenie a ochranou obchodného tajomstva.

Ďalší spor sa týkal pseudonymizovaných údajov a pojmu osobných údajov. Išlo o prípad EDPS proti Single Resolution Board (C-413/23 P, 4.9.2025).

V rámci riešenia krízy Banco Popular Español umožnil SRB (Single Resolution Board - orgán EÚ zodpovedný za riešenie kríz bánk v európskom bankovom spektre) dotknutým akcionárom a veriteľom predkladať pripomienky. Tieto pripomienky SRB spracoval a časť z nich – v pseudonymizovanej forme poskytol externému konzultantovi (spoločnosti Deloitte), ktorý mal slúžiť na posúdenie finančných dopadov. Niektoré osoby napadli tento prenos údajov tým, že SRB ich dostatočne neinformoval, že ich údaje môžu byť odovzdané tretej strane. Európsky dozorný úradník pre ochranu údajov (EDPS) tvrdil, že ide o osobné údaje a uložil regulačnému orgánu sankciu za porušenie GDPR. Národný súd rozhodnutie EDPS zrušil, ale SDEÚ rozhodol, že:

- pseudonymizované údaje zostávajú osobnými údajmi pre subjekt, ktorý disponuje prostriedkami na ich re-identifikáciu, pretože vie údaje opäť priradiť ku konkrétnym osobám,

- pre tretie strany, ktoré nemajú realistické prostriedky na identifikáciu jednotlivcov, pseudonymizované dáta nemusia byť osobnými údajmi. Posúdenie sa má robiť z perspektívy príjemcu v čase prenosu, nie teoretickej možnosti získať ďalšie údaje.

Záverom tejto časti možno poukázať na jedno vnútroštátne rozhodnutie, týkajúce sa likvidácie dokumentov obsahujúcich osobné údaje (sp. zn. 8Co/29/2025, 4.9.2025).

Ide o rozhodnutie Krajského súdu v Prešove vo veci porušenia ochrany osobných údajov klientov spoločnosti Orange Slovensko, a.s., pri likvidácii dokumentov obsahujúcich citlivé údaje, ako meno, adresa, rodné číslo, číslo občianskeho preukazu, telefónne číslo či podpis. Úrad na ochranu osobných údajov potvrdil, že spoločnosť nepostupovala s primeranou starostlivosťou.
Žalobca sa preto domáhal náhrady nemajetkovej ujmy za neoprávnené sprístupnenie svojich údajov. Okresný súd mu priznal 3 300 €, odvolací súd sumu znížil na 110 €, no potvrdil zásah do jeho práv. V konečnom rozhodnutí Krajský súd zdôraznil, že aj menší zásah predstavuje porušenie základného práva na ochranu osobných údajov podľa GDPR a priznal žalobcovi plnú náhradu trov konania. Súd odmietol aplikovať moderáciu trov v prospech porušovateľa, keďže by to bolo v rozpore so zásadou spravodlivosti a oslabilo by ochranu súkromia a osobných údajov občanov.

KURZY A EVENTY

Dňa **8. októbra 2025** sa v Bukurešti bude konať konferencia **CRA - Making the EU Market Resilient.**

Organizuje ju ENISA v partnerstve s Rumunským národným riaditeľstvom pre kybernetickú bezpečnosť (DNSC) a Európskym centrom a sieťou kompetencií pre kybernetickú bezpečnosť (ECCC). Podujatie sa zameriava na Cyber Resilience Act, ktorý nadobudol účinnosť 10. decembra 2024. CRA zavádza požiadavky na kybernetickú bezpečnosť pre produkty s digitálnymi prvkami ako podmienku prístupu na trh EÚ a vyžaduje, aby ich výrobcovia uplatňovali počas celého životného cyklu produktu. Ide o prvé podujatie Európskej únie, ktoré spája relevantných aktérov z celého spektra odolnosti produktov s digitálnymi prvkami dostupných na jednotnom trhu EÚ. Jeho cieľom je ochrana občanov a podnikov EÚ, vrátane malých a stredných podnikov (MSP), a podpora bezpečného digitálneho jednotného trhu EÚ.

- **viac informácií TU**

Dňa **30. októbra 2025** sa v Bruseli bude konať konferencia **EdTech** 2025.

Nadväzujúc na závery svojho prvého ročníka z roku 2024, konferencia EIT EdTech 2025 spája kľúčových aktérov z oblasti vzdelávania a inovácií – vrátane lídrov v odvetví, startupov, zástupcov verejného sektora, univerzít a škôl. Jej zámerom je hľadať synergie, zdieľať osvedčené postupy a diskutovať o politikách, ktoré sú kľúčové pre podporu inovácií s reálnym dopadom v digitálnom vzdelávaní.

- **viac informácií TU**

Dňa **3 až 4. novembra 2025** sa v Kodani bude konať **AI in Science Summit,** ktorý spojí vedcov, lídrov z priemyslu, investorov a tvorcov politík s cieľom preskúmať, ako umelá inteligencia transformuje výskum a ako môže byť Európa v tomto smere zodpovedným lídrom. Podujatie sa začne pohľadom na transformačnú silu AI vo vede a na osobitý prístup Európy k inováciám.

- **viac informácií TU**

LITERATÚRA

Do pozornosti dávame najnovšiu správu agentúry ENISA o prostredí hrozieb – **Threat Landscape 2025** (z októbra 2025), ktorá analyzuje 4 875 kybernetických incidentov v celej EÚ. Správa potvrdzuje, že kybernetický priestor EÚ čelí bezprecedentnému tlaku, pričom počet a sofistikovanosť útokov rastie. Analyzovaná vzorka **4 875 incidentov** (od júla 2024 do júna 2025) odhalila nasledujúce hlavné trendy: ransomvér, DDoS útoky a sociálne inžinierstvo.

- **viac TU**

Organizácia **Future of Privacy Forum** monitorovala 210 legislatívnych návrhov v 42 štátoch. Správa o stave legislatívnych prístupov jednotlivých štátov k AI v roku 2025 identifikovala kľúčové trendy v oblasti vývoja a nasadzovania umelej inteligencie v súkromnom sektore.

- **viac TU**

Európska komisia vydala novú štúdiu s názvom „**The Impact of Human-AI Interaction on Discrimination**", ktorej autori spochybňujú bežný predpoklad v oblasti riadenia AI, že samotný ľudský dohľad dokáže zabrániť algoritmickej diskriminácii.

S využitím kombinovanej výskumnej metodiky a údajov od vyše 1 400 personalistov a bankových odborníkov v Taliansku a Nemecku výskumníci zistili, že ľudia vykonávajúci dohľad sa rovnako pravdepodobne riadia zaujatými odporúčaniami od bežnej AI, ako aj od tej, ktorá bola naprogramovaná na dodržiavanie férovosti. Dokonca aj v prípadoch, keď „férová" AI znížila mieru rodových predsudkov, konečné výsledky boli stále ovplyvnené vlastnými, už existujúcimi predsudkami ľudí, ktorí rozhodovali. Rozhovory odhalili, že účastníci často uprednostňovali záujmy spoločnosti pred férovosťou.

Záver? Samotný ľudský dohľad nestačí. Regulátori a tvorcovia politík budú musieť navrhnúť rámce systémového dohľadu, ktoré budú obsahovať jasné pravidlá určujúce, kedy a akým spôsobom by mali ľudia zasahovať do rozhodnutí AI alebo ich meniť.

- **viac TU**

Európska komisia tiež zverejnila prvú správu Odbornej skupiny pre podmorské káble (Cables Expert Group), ktorá zahŕňa mapovanie existujúcich a plánovaných podmorských dátových káblov, koordinované posúdenie rizík so siedmimi kľúčovými scenármi hrozieb a usmernenia na záťažové testovanie týchto rizík.

Správa, vypracovaná v spolupráci s členskými štátmi a agentúrou ENISA, taktiež ponúka podrobný prehľad politík a trhu v oblasti infraštruktúr podmorských káblov EÚ.

Spolu so správou Komisia oznámila nové financovanie v rámci programu Digitálna Európa na zriadenie regionálnych káblových uzlov a ďalšie testovanie odolnosti podmorských káblových sietí, čím sa posilňuje strategická digitálna chrbtica Európy.
- **viac TU**

Za pozornosť stojí aj najnovší príspevok do sympózia *Competition Corner* na portáli *EU Law Live* komplexnú analýzu meniaceho sa prostredia presadzovania pravidiel podľa Aktu o digitálnych trhoch (DMA) a Aktu o digitálnych službách (DSA). Autori Peter Hense a Rosalia Anna D'Agostino zdôrazňujú, že hoci Digital Services Act (DSA) a Digital Markets Act (DMA) patria k hlavným európskym nariadeniam digitálneho balíka, ich úloha v súkromnom presadzovaní práv sa musí chápať odlišne. Oba akty síce posilňujú opatrenia v digitálnom priestore, no každý z nich cieľuje na iné výsledky, keď ide o účasť súkromných aktérov pri presadzovaní pravidiel proti veľkým online platformám.
- **viac TU**

Európska komisia predstavila taktiež rámec na klasifikáciu upravených modelov umelej inteligencie na všeobecné účely (GPAI) ako „nových modelov" na základe zmien v ich správaní.
Upravený model GPAI by sa mal v zmysle aktu o umelej inteligencii považovať za úplne nový systém. Správa stanovuje dva spôsoby, ako hodnotiť zmenu správania: primárne priamym porovnaním schopností alebo výstupov, alebo prostredníctvom zástupných ukazovateľov (proxy metrík), ako sú výpočtový výkon a využitie dát.
- **viac TU**

Microsoft zverejnil svoj **Digital Defense Report 2025**. Vydanie výročnej správy spoločnosti Microsoft o digitálnej obrane na rok 2025 prináša zásadný prehľad o aktuálnej situácii v oblasti kybernetických hrozieb a o vyvíjajúcich sa stratégiách obrany. Report analyzuje údaje a bezpečnostné signály z júla 2024 až júna 2025 a vychádza z miliárd spracovaných bezpečnostných dát.

Správa ukazuje, že kybernetické hrozby sú stále komplexnejšie a rozsiahlejšie, pričom sa čoraz viac zameriavajú na finančný zisk a exfiltráciu citlivých dát, a vyžaduje nové prístupy k obrane, najmä v kontexte umelej inteligencie (AI) a identít. Viac ako polovica kyberútokov s identifikovaným motívom bola zameraná na vydieranie a ransomware, pričom 80 % incidentov vyšetrených tímami Microsoftu zahŕňalo krádež alebo únik dát.
- **viac TU**

Ďalší report s názvom **„Digital Monitoring, Algorithmic Management and the Platformisation of Work in Europe"** vydaný pod záštitou Európskej komisie sa zameriava na to, ako digitálne technológie a umelá inteligencia menia podobu práce v Európe.

Na základe prieskumu AIM-WORK z rokov 2024 – 2025 výsledky ukazujú, že viac ako 90 % pracovníkov v EÚ v súčasnosti používa digitálne zariadenia a čo je podstatné, každý tretí už využíva nástroje AI.

- **viac TU**